


FORM PTO-1396 (REV. 10-2000)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY'S DOCKET NUMBER <div style="border: 1px solid black; padding: 2px; text-align: center;">6400-11WOUS</div>	
<b>TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371</b>				U.S. APPLICATION NO. (Indicate by 37 CFR 1.9)	
<div style="border: 1px solid black; padding: 2px; font-size: 1.5em; font-weight: bold;">097720353</div>					
INTERNATIONAL APPLICATION NO. PCT/DE00/01086		INTERNATIONAL FILING DATE April 7, 2000		PRIORITY DATE CLAIMED April 30, 1999	
TITLE OF INVENTION SIGNING AND SIGNATURE CHECKING OF MESSAGES					
APPLICANT(S) FOR DO/EO/US <div style="text-align: center;">Michael Noite</div>					
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:					
<ol style="list-style-type: none"> <li>1. <input checked="" type="checkbox"/> This is a <b>FIRST</b> submission of items concerning a filing under 35 U.S.C. 371.</li> <li>2. <input type="checkbox"/> This is a <b>SECOND</b> or <b>SUBSEQUENT</b> submission of items concerning a filing under 35 U.S.C. 371.</li> <li>3. <input checked="" type="checkbox"/> This is an express request to promptly begin national examination procedures (35 U.S.C. 371(f)).</li> <li>4. <input checked="" type="checkbox"/> The US has been elected by the expiration of 19 months from the priority date (PCT Article 31).</li> <li>5. <input checked="" type="checkbox"/> A copy of the International Application as filed (35 U.S.C. 371(c)(2))           <ol style="list-style-type: none"> <li>a. <input type="checkbox"/> is attached hereto (required only if not communicated by the International Bureau).</li> <li>b. <input checked="" type="checkbox"/> has been communicated by the International Bureau.</li> <li>c. <input type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US).</li> </ol> </li> <li>6. <input checked="" type="checkbox"/> An English language translation of the International Application as filed (35 U.S.C. 371(c)(3)).</li> <li>7. <input checked="" type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19(35 U.S.C. 371(c)(3))           <ol style="list-style-type: none"> <li>a. <input type="checkbox"/> are attached hereto (required only if not communicated by the International Bureau).</li> <li>b. <input type="checkbox"/> have been communicated by the International Bureau.</li> <li>c. <input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired.</li> <li>d. <input checked="" type="checkbox"/> have not been made and will not be made.</li> </ol> </li> <li>8. <input type="checkbox"/> An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).</li> <li>9. <input checked="" type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).</li> <li>10. <input type="checkbox"/> An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).</li> </ol>					
<b>Items 11 to 16 below concern document(s) or information included:</b>					
<ol style="list-style-type: none"> <li>11. <input checked="" type="checkbox"/> An Information Disclosure Statement under 37 CFR 1.97 and 1.98.</li> <li>12. <input checked="" type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.</li> <li>13. <input checked="" type="checkbox"/> A FIRST preliminary amendment.  <input type="checkbox"/> A SECOND or SUBSEQUENT preliminary amendment.</li> <li>14. <input type="checkbox"/> A substitute specification.</li> <li>15. <input type="checkbox"/> A change of power of attorney and/or address letter.</li> <li>16. <input checked="" type="checkbox"/> Other items or information: <span style="margin-left: 20px;">Form PCT/IB/308</span></li> </ol>					
<div style="text-align: right;">           EXPRESS MAIL™ MAILING LABEL            Number <u>EL 202034908/US</u>            Date of Deposit <u>December 21, 2000</u>            I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office To Addressee" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to Box PCT, Commissioner of Patents and Trademarks, Washington, D.C. 20231  <u>J. R. Holdsworth</u>            (Typed Name of Person Mailing Paper or Fee)              (Signature of Person Mailing Paper or Fee)         </div>					

U.S. APPLICATION NO. <b>03/720553</b> INTERNATIONAL APPLICATION NO. <b>PCT/DE00/01086</b>		ATTORNEY'S DOCKET NUMBER <b>6400-11WOUS</b>																																											
17. <input checked="" type="checkbox"/> The following fees are submitted: <b>BASIC NATIONAL FEE (37 CFR 1.492(a)(1)-(5)):</b> Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO ..... <b>\$1000.00</b> International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO ..... <b>\$860.00</b> International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO ..... <b>\$710.00</b> International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) ..... <b>\$690.00</b> International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfy provisions of PCT Article 33(1)-(4) ..... <b>\$100.00</b> <b>ENTER APPROPRIATE BASIC FEE AMOUNT = \$ 860.00</b>		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 60%;">CALCULATIONS</th> <th style="width: 40%;">PTO USE ONLY</th> </tr> <tr> <td colspan="2" style="height: 100px;"></td> </tr> </table>		CALCULATIONS	PTO USE ONLY																																								
CALCULATIONS	PTO USE ONLY																																												
Surcharge of <b>\$130.00</b> for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(e)).		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 40%;">CLAIMS</th> <th style="width: 20%;">NUMBER FILED</th> <th style="width: 20%;">NUMBER EXTRA</th> <th style="width: 20%;">RATE</th> <th style="width: 10%;">\$</th> <th style="width: 10%;"></th> </tr> <tr> <td>Total claims</td> <td>10 - 20 =</td> <td>-</td> <td>X \$18.00</td> <td>\$</td> <td></td> </tr> <tr> <td>Independent claims</td> <td>2 - 3 =</td> <td>-</td> <td>X \$80.00</td> <td>\$</td> <td></td> </tr> <tr> <td colspan="3">MULTIPLE DEPENDENT CLAIM(S) (if applicable)</td> <td>+ \$270.00</td> <td>\$</td> <td></td> </tr> <tr> <td colspan="4"><b>TOTAL OF ABOVE CALCULATIONS =</b></td> <td><b>\$ 860.00</b></td> <td></td> </tr> </table>		CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	\$		Total claims	10 - 20 =	-	X \$18.00	\$		Independent claims	2 - 3 =	-	X \$80.00	\$		MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ \$270.00	\$		<b>TOTAL OF ABOVE CALCULATIONS =</b>				<b>\$ 860.00</b>													
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	\$																																									
Total claims	10 - 20 =	-	X \$18.00	\$																																									
Independent claims	2 - 3 =	-	X \$80.00	\$																																									
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ \$270.00	\$																																									
<b>TOTAL OF ABOVE CALCULATIONS =</b>				<b>\$ 860.00</b>																																									
<input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="4"><b>SUBTOTAL =</b></td> <td><b>\$ 860.00</b></td> <td></td> </tr> <tr> <td colspan="2" style="vertical-align: top;">         Processing fee of <b>\$130.00</b> for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30          months from the earliest claimed priority date (37 CFR 1.492(f)).       </td> <td colspan="2"></td> <td>\$</td> <td></td> </tr> <tr> <td colspan="4"><b>TOTAL NATIONAL FEE =</b></td> <td><b>\$ 860.00</b></td> <td></td> </tr> <tr> <td colspan="2" style="vertical-align: top;">         Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be          accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). <b>\$40.00</b> per property       </td> <td colspan="2"></td> <td>\$</td> <td>40.00</td> </tr> <tr> <td colspan="4"><b>TOTAL FEES ENCLOSED =</b></td> <td><b>\$ 900.00</b></td> <td></td> </tr> <tr> <td colspan="4"></td> <td>Amount to be refunded:</td> <td>\$</td> </tr> <tr> <td colspan="4"></td> <td>charged:</td> <td>\$</td> </tr> </table>		<b>SUBTOTAL =</b>				<b>\$ 860.00</b>		Processing fee of <b>\$130.00</b> for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				\$		<b>TOTAL NATIONAL FEE =</b>				<b>\$ 860.00</b>		Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). <b>\$40.00</b> per property				\$	40.00	<b>TOTAL FEES ENCLOSED =</b>				<b>\$ 900.00</b>						Amount to be refunded:	\$					charged:	\$
<b>SUBTOTAL =</b>				<b>\$ 860.00</b>																																									
Processing fee of <b>\$130.00</b> for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				\$																																									
<b>TOTAL NATIONAL FEE =</b>				<b>\$ 860.00</b>																																									
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). <b>\$40.00</b> per property				\$	40.00																																								
<b>TOTAL FEES ENCLOSED =</b>				<b>\$ 900.00</b>																																									
				Amount to be refunded:	\$																																								
				charged:	\$																																								
a. <input checked="" type="checkbox"/> A check in the amount of <u>\$ 900.00</u> to cover the above fees is enclosed.  b. <input type="checkbox"/> Please charge my Deposit Account No. <u>13-0235</u> in the amount of \$_____ to cover the above fees. A duplicate copy of this sheet is enclosed.  c. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. <u>13-0235</u> . A duplicate copy of this sheet is enclosed.																																													
<b>NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.</b>																																													
SEND ALL CORRESPONDENCE TO:  Donald K. Huber McCormick, Paulding & Huber LLP CityPlace II 185 Asylum Street Hartford, CT 06103-3402																																													
<div style="text-align: right;">           SIGNATURE:          Donald K. Huber Dec. 21, 2000          NAME          18,686          REGISTRATION NUMBER       </div>																																													

"EXPRESS MAIL" MAILING LABEL  
NUMBER EL702049080US  
DATE OF DEPOSIT December 21, 2000  
I HEREBY CERTIFY THAT THIS PAPER OR FEE IS BEING DEPOSITED  
WITH THE UNITED STATES POSTAL SERVICE "EXPRESS MAIL POST  
OFFICE TO ADDRESSEE" SERVICE UNDER 37 C.F.R. 1.10 ON THE  
DATE INDICATED ABOVE AND IS ADDRESSED TO THE  
COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON,  
D. C. 20231

J. R. Holdsworth  
(TYPED NAME OF PERSON MAILING PAPER OR FEE)

J. R. Holdsworth  
(SIGNATURE OF PERSON MAILING PAPER OR FEE)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In the Application of )  
for SIGNING AND SIGNATURE CHECKING )  
OF MESSAGES )  
Serial No: National Stage Entry of International ) Our Docket No: 6400-11WOUS  
Application No. PCT/DE00/01086 filed April 7, 2000 )  
Filed: Simultaneously herewith )

Hartford, Connecticut, December 21, 2000

**Box PCT**  
Assistant Commissioner for Patents  
Washington, D. C. 20231

**PRELIMINARY AMENDMENT**

S I R:

Concurrently with the entry of the above-identified international application into  
the U.S. National Stage, please amend it as follows:

In the Specification (of the English Translation of the Application)

Page 1, line 3, delete the sub-heading "Technical field" and substitute --FIELD  
OF THE INVENTION--.

Page 1, line 8, delete the sub-heading "Prior art" and substitute --  
BACKGROUND OF THE INVENTION--.

Page 2, line 15, delete the sub-heading "Description of the invention" and  
substitute --SUMMARY OF THE INVENTION--.

Page 3, lines 13 and 14, delete the sub-heading "Description of at least one embodiment at least of the invention" and substitute --DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS--.

In the Claims (of the English Translation of the Application)

Claim 5 - amend as follows:

5. (Amended) The method as claimed in claim 1, wherein the sequence number is produced by a pseudo-random number generator.

Claim 6 - amend as follows:

6. (Amended) The method as claimed in claim 1, wherein the encryption of the sequence number by means of the main key is used as the one-time encryption.

Claim 7 - amend as follows:

7. (Amended) The method as claimed in claim 1, wherein the control center (10) produces a number of signing keys (14) in advance, and transmits them to the sender (30), possibly together with the associated sequence numbers (12).

Claim 8 - amend as follows:

8. (Amended) The method as claimed in claim 1, wherein the receiver (30) maintains a list of already used sequence numbers, and rejects already used sequence numbers.

Claim 10 - amend as follows:

10. (Amended) The device as claimed in claim 9, wherein a generator using a deterministic method produces one or more sequence numbers corresponding to the number of checks.

In the Abstract

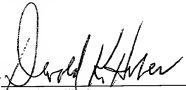
Delete the sub-heading "Abstract" and substitute --Abstract of the Disclosure--;  
and on the last line, delete "Figure 1".

REMARKS

The above amendments are requested to put the application into better U.S. format and to delete multiple dependencies.

Any fee required by the filing of this amendment may be charged to our Deposit Account No. 13-0235.

Respectfully submitted,

By   
Donald K. Huber  
Registration No. 18,686  
Attorney for Applicant

McCormick, Paulding & Huber LLP  
CityPlace II  
185 Asylum Street  
Hartford, Connecticut 06103-4102  
(860) 549-5290

09/720353  
528 R354 PCT/PTO 21 DEC 2000

U. S. National Stage Entry of Int'l. Appln. No. PCT/DE00/01086

*Attorney Docket No. 6400-11WOUS*

99P6221)

**ENGLISH TRANSLATION OF THE APPLICATION**

09  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199  
2200  
2201  
2202  
2203  
2204

**Signing and signature checking of messages**Technical field

- 5 The invention relates to the signing and signature checking of messages using secret keys.

Prior art

- 10 In order to provide protection against corruption of messages, it is known for symmetrical cryptography to be used to form a signature by means of which the receiver can check, with very high probability, whether the message has been transmitted without corruption and  
15 originates from the predetermined sender. However, one precondition is that the sender and receiver have a common, secret key, which must be stored in secure form. One such method is described, for example, in Patent Specification US 4,549,075.

- 20 Symmetrical cryptography, in particular the DES method, is frequently used in smart cards, because this method can be programmed very efficiently. The smart cards furthermore have a read only memory in which a main key  
25 is stored in secure and secret form, and this main key is also stored in secure form in a control center.

- If it is now intended to send a message, protected against corruption, from a sender to the receiver, in  
30 this case the smart card, then, until now, the sender has had to have the message signed by the control center, since the control center cannot provide the sender with the secret main key



without weakening the entire system. Furthermore, measures are required to ensure that the message is protected against corruption and imitation of a legitimate sender during transmission from the sender  
5 to the main center.

The object of the invention is thus to specify a method for corruption protection of messages by means of a signature which can be formed by a sender and can be  
10 sent to a receiver without the sender having the secret main key, which is shared by the receiver and a control center, or without the message having to be sent in advance to the control center, for signature formation.

15 Description of the invention

The invention uses a method in which the control center forms signing keys in advance, and provides them to the sender. As is described in more detail in the exemplary  
20 embodiments, the receiver can model the signing key, and can thus check the message.

This relates to a method for signing a message, in which a control center and the receiver have a  
25 permanent, common main key. The control center produces a sequence number in advance, and produces a signing key from this by means of a one-time function. Both are provided to the sender, in secure form. The sender uses the signing key to form a signature for the message,  
30 and sends this signature with the sequence number and the message to the receiver. The receiver uses a one-time function, main key and sequence number to form a check key, and thus checks the signature on the message.

Further features and advantages of the invention result from the following description, which explains the invention with reference to an exemplary embodiment and in conjunction with the attached drawing.

5

Brief description of the drawing

In the figures:

- 10 Figure 1 shows a diagram in which the data flow is symbolized, with the components involved.

Description of at least one embodiment at least of the invention

15

Figure 1 indicates the three parties involved in the method, namely the control center 10, the sender 20 and the receiver 30, separated by dashed-dotted lines.

- 20 The control center 10 contains a secure memory 11 for a secret key which is otherwise used, for example, in a symmetrical cryptographic encryption or signing method. The receiver 30 contains a corresponding memory 11', which contains the same key. This key is written to the
- 25 control center during initialization, for example, if the receiver 30 is a smart card. Otherwise, key distribution methods known from cryptography can be used. In this case, the key is stored only once or at very long time intervals; the storage can be regarded
- 30 as being permanent for the method according to the invention.

The control center 10 furthermore contains a sequence generator 12. This provides a series of numbers, which each differ. In the simplest case, this is a sequential number. However, it is better to use a known pseudo-random number generator, for example using the modulo method. If the parameters are chosen correctly, these pseudo-random number generators produce a sequence of new numbers in each case until the cycle which is governed by the modulus has been run through.

5 Decreasing numbers or numbers with a step interval greater than unity can also be used. It is likewise possible to use the date and time as a unique sequence number, possibly as the number of seconds since an appointed start.

10

15 The control center thus produces one or more sequence numbers 12. A one-time encrypter 13 uses the main key to form a signing key 14 from such a sequence number 12. This is most easily done by the sequence number 12 being encrypted by means of the main key. In this case, a short sequence number is filled out by means of further data to the block length of the encryption method. Although binary zeros can be used for this purpose, it is better to use a function of the sequence number, for example its square. It is also possible to use a constant text, which does not consist of binary zeros and is kept confidential. Since the block size is generally in the same order of magnitude as the key length, it is still possible to use the result as a

20

25 key; if necessary, bits must be added or the number of bits reduced by convolution.

30

The essential characteristic of the one-time encrypter is that it is virtually impossible to deduce the main

key. Although the method just described is not a one-time encryption since, for example, the receiver could form the sequence number from the signing key by decryption, the "one-time" functionality is the main feature.

Other one-time functions are thus used in other embodiments which link the main key and the sequence number in a reproducible manner to form a signing key without anyone who does not have the main key relating to a given sequence number being able to form a valid signing key, or vice versa, or being able to determine the main key from the signing key and the sequence number. Such methods are generally referred to as "message authentication codes" (MAC). One such method may be formed, in particular, by applying any desired cryptographically secure one-time function to a combination of a main key and sequence number. A concatenation, exclusive-OR, multiplication with or without modulo formation or addition, etc., may be used as the combination.

The control center 10 thus provides one or more pairs of sequence numbers 12, and signing keys 14 produced from them. This can be done, for example, by printing out on security paper, by storage in a further smart card or by some other secure data transmission. These pairs are provided to the sender 20 in advance, who must store them in a secure and confidential manner.

The sender 20 who wishes to send a message 21 to the receiver 30 takes a pair of sequence numbers 12 and signing keys 14 and uses the signer 24 to determine the signature for the message 21. The DES method, for example

in accordance with ANSI X9.9, is preferably also used in this case. Alternatively, a signature can be produced by a combination of a cryptographic hash function and a message authentication code. Methods  
5 relating to this have been described frequently and comprehensively in the cryptographic literature.

The sender then forms a data set 22, which contains three fields with the sequence number 22a, the message  
10 22b and the signature 22c. The signing key 14 which has just been used is deleted.

The data set 22 is now transmitted to the receiver 30, which thus receives a data set 22' which once again  
15 contains three fields, which are regarded as the sequence number 22a', the message 22b' and the signature 22c'. Normally, this data set has already been protected against transmission errors by other security or plausibility mechanisms.

20 The receiver extracts the sequence number 22a' from the received data set 22', and passes this together with the main key 11' to one-time encryption 13' which, in the same way as the one-time encryption 13, is located  
25 in the control center 10 and is functionally identical to it. A check key 14' is produced at the output of the one-time function. If the sequence number has been transmitted correctly, this check key 14' is identical to the signing key 14 which the sender 20 has used. The  
30 check key 14' is passed to a signature checker 38 together with the message 22b' which has arrived and the signature 22c' which has arrived. If all three match one another, an enable signal for further use of the message is produced at the output of the signature  
35 checker 38. At the end of the check, the check key 14' is destroyed, irrespective of the result.

In one development of the invention, the receiver maintains a list of already used sequence numbers, and rejects messages with already used sequence numbers. This provides additional security against misuse.

5

Since the sequence number is preferably produced by a deterministic generator, there is no need to transmit the sequence number. Since the common main key has to be transmitted in a secure environment to the receiver  
10 in any case, the initial value of the generator can be transmitted at the same time. Whenever a message is received, the receiver produces a new value for the sequence number, and thus forms the check key 14' without the sequence number having to be transmitted as  
15 well. In order to be robust against double transmissions and lost messages, one of the last and following sequence numbers is expediently also then used. In this case as well, the control center can provide the sender with a number of signing keys 14,  
20 which the sender should then use in the predetermined sequence.

One possible application of the invention is in the field of automatic cash dispensers. The control center  
25 is in this case the bank control center, which uses a main key for checking the PIN and supplies personalized checking modules to the manufacturer of automatic cash dispensers in the control center. The sender may be a manufacturer or a local bank organization which, for  
30 example, wishes to load a currency conversion rate or a discount rate into the automatic cash dispensers; however, such organizations cannot introduce their own secret key into the cash dispenser, nor do they wish to install their own security module.

If the receiver does not contain a non-volatile memory, the receiver can also produce the sequence numbers from the start and test the signature with each of them. The loss of security in this case is low, but this does not  
5 provide any protection against double use.

**Patent Claims**

1. A method for signing a message (22) by a sender (20), and for checking the signature by a receiver, wherein a control center (10) and a receiver (30) have a secret, common main key (11, 11'), having the following features:
- the control center (10)
    - \* produces a sequence number (12) and
    - 10 \* from this and using the main key (11) produces a signing key (14) by means of one-time encryption (13), and
    - \* provides the sender with the signing key (14);
  - 15 - the sender (20)
    - \* uses the signing key (14) to form a signature (22c) for the message (21, 22c) and
    - \* sends to the receiver a message set (22) which contains at least the message (22b) and the signature (22c).
  - 20 - The receiver (30)
    - \* determines the sequence number (22a'),
    - \* forms the one check key (14') using the one-time encryption (13') and the main key (11'), and
    - 25 \* uses this to check the signature (22c) on the message.
2. The method as claimed in claim 1, wherein the sequence number (12, 22a, 22a') is transmitted together with the signing key (14) from
- 30



the control center to the sender (20), and is transmitted from the sender (20) via the data set (22, 22') to the receiver.

- 5     3. The method as claimed in claim 1, wherein the sequence number (12) is produced by a generator in synchronism with the number of signing and check keys used in the control center (10) and in the receiver.
- 10    4. The method as claimed in claim 1, wherein the sequence number (12) is produced by a generator in synchronism with the number of signing and check keys used in the control center (10) and in the sender, and is transmitted via the data set (22, 22') to the receiver.
- 15    5. The method as claimed in one of the preceding claims, wherein the sequence number is produced by a pseudo-random number generator.
- 20    6. The method as claimed in one of the preceding claims, wherein the encryption of the sequence number by means of the main key is used as the one-time encryption.
- 25    7. The method as claimed in one of the preceding claims, wherein the control center (10) produces a number of signing keys (14) in advance, and transmits them to the sender (30), possibly together with the associated sequence numbers (12).
- 30    8. The method as claimed in one of the preceding claims, wherein the receiver (30) maintains a list of already used sequence numbers, and rejects already used sequence numbers.

9. A device for signing a message (22, 22') which is sent from a sender (20) to a receiver (30), having the following features:
- 5       - a control center (10) and the receiver (30) have a first and a second memory for a secret, common main key (11, 11');  
10       - in the control center (10), one input of a first one-time encrypter (13) is connected to the first protected memory (11), and another input is connected to a generator (12) for a sequence number,  
15       - the output of the one-time encrypter (13) is connected to the sender (20) via a transport medium,  
20       - a signature generator (24) is provided in the sender, and its inputs are connected to the output of the one-time encrypter and to the message (21, 22b) to be signed,  
25       - the output of the signature generator (24) is connected to a device which assembles at least the signature (22c) and the message (22b) to form a message block (22) and whose output is connected to the receiver (30) via a transport medium,  
30       - a signature checker (22') is provided in the receiver, whose inputs are connected firstly to the message (22b') and to the signature (22c) of the message block (22') which has arrived via the transport medium,  
      - and secondly to the output of a second one-time encrypter (13'), whose inputs are connected firstly to the second memory (11') for the



## Abstract

Method for signing a message, in which a control center and the receiver have a permanent, common main key. The control center produces a sequence number in advance, and a signing key from this by means of a one-time function. Both are provided in secure form to the sender. The sender uses the signing key to form a signature for the message, and sends the signature, with the sequence number and the message, to the receiver. The receiver uses a one-way function, main key and sequence number to form a check key, and thus checks the signature on the message.

Figure 1

99P6221

- 10 -

the control center to the sender (20), and is transmitted from the sender (20) via the data set (22, 22') to the receiver.

3. The method as claimed in claim 1, wherein the sequence number (12) is produced by a generator in synchronism with the number of signing and check keys used in the control center (10) and in the receiver.
4. The method as claimed in claim 1, wherein the sequence number (12) is produced by a generator in synchronism with the number of signing and check keys used in the control center (10) and in the sender, and is transmitted via the data set (22, 22') to the receiver.
5. <sup>(Amended)</sup> The method as claimed in <sup>CLAIM 1</sup> ~~one of the preceding claims~~, wherein the sequence number is produced by a pseudo-random number generator.
6. <sup>(Amended)</sup> The method as claimed in <sup>CLAIM 1</sup> ~~one of the preceding claims~~, wherein the encryption of the sequence number by means of the main key is used as the one-time encryption.
7. <sup>(Amended)</sup> The method as claimed in <sup>CLAIM 1</sup> ~~one of the preceding claims~~, wherein the control center (10) produces a number of signing keys (14) in advance, and transmits them to the sender (30), possibly together with the associated sequence numbers (12).
8. <sup>(Amended)</sup> The method as claimed in <sup>CLAIM 1</sup> ~~one of the preceding claims~~, wherein the receiver (30) maintains a list of already used sequence numbers, and rejects already used sequence numbers.

secret main key and to a means for providing a  
(Amended) sequence number (22a').

10. The device as claimed in claim 9, wherein a  
generator produces the sequence number (22a')  
5 using a deterministic method ~~thereby~~ one or more  
sequence numbers corresponding to the number of  
checks.

1/1

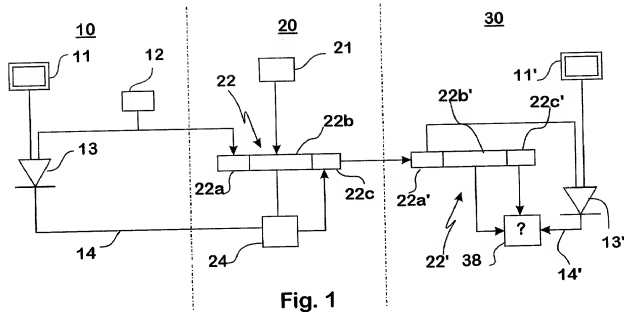


Fig. 1

# Declaration and Power of Attorney For Patent Application

## Erklärung und Vollmacht für Patentanmeldungen

### German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

As a below named inventor, I hereby declare that:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

My residence, post office address and citizenship are as stated below next to my name,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Signierung und Signaturprüfung von  
Nachrichten

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

deren Beschreibung

the specification of which

(zutreffendes ankreuzen)

☐ hier beigelegt ist.

(check one)

☐ is attached hereto.

☒ am 07.04.2000 als

☐ was filed on \_\_\_\_\_ as

PCT internationale Anmeldung

PCT international application

PCT Anmeldungsnummer PCT/DE00/01086

PCT Application No. \_\_\_\_\_

eingereicht wurde und am \_\_\_\_\_

and was amended on \_\_\_\_\_

abgeändert wurde (falls tatsächlich abgeändert).

(if applicable)

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:



# German Language Declaration

Prior foreign applications  
Priorität beansprucht

Priority Claimed

19919909.4 Germany 30 April 1999  
(Number) (Country) (Day Month Year Filed)  
(Nummer) (Land) (Tag Monat Jahr eingereicht)

☒ ☐  
Yes No  
Ja Nein

\_\_\_\_\_  
(Number) (Country) (Day Month Year Filed)  
(Nummer) (Land) (Tag Monat Jahr eingereicht)

☐ ☐  
Yes No  
Ja Nein

\_\_\_\_\_  
(Number) (Country) (Day Month Year Filed)  
(Nummer) (Land) (Tag Monat Jahr eingereicht)

☐ ☐  
Yes No  
Ja Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.)  
(Anmeldeseriennummer)

(Filing Date)  
(Anmeldedatum)

(Status)  
(patentiert, anhängig,  
aufgegeben)

(Status)  
(patentiert, pending,  
abandoned)

(Application Serial No.)  
(Anmeldeseriennummer)

(Filing Date)  
(Anmeldedatum)

(Status)  
(patentiert, anhängig,  
aufgegeben)

(Status)  
(patentiert, pending,  
abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden können, und dass derartige wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

# German Language Declaration

VERRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: (Name und Registrationsnummer anführen)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Attorneys of the firm of McCormick, Paulding & Huber LLP as shown on the attached list

Telefongespräche bitte richten an:  
(Name und Telefonnummer)

Direct Telephone Calls to: (name and telephone number)

Donald K. Huber (860) 549-5290

Postanschrift:

Send Correspondence to:

Donald K. Huber

Voller Name des einzigen oder ursprünglichen Erfinders		Full name of sole or first inventor:	
NOLTE, Michael			
Unterschrift des Erfinders	Datum	Inventor's signature	Date
<i>Michael Nolte</i>	31.10.2000		
Wohnsitz		Residence	
D-33034 Brakel, Deutschland		DEX	
Staatsangehörigkeit		Citizenship	
deutsch			
Postanschrift		Post Office Address	
Koberg Weg 2a			
D-33034 Brakel			
Deutschland			
Voller Name des zweiten Miterfinders (falls zutreffend):		Full name of second joint inventor, if any:	
Unterschrift des Erfinders	Datum	Second inventor's signature	Date
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).

Voller Name des dritten Miterfinders:		Full name of third joint inventor:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	
Voller Name des vierten Miterfinders (falls zutreffend):		Full name of fourth joint inventor, if any:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	
Voller Name des fünften Miterfinders (falls zutreffend):		Full name of fifth joint inventor, if any:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	
Voller Name des sechsten Miterfinders (falls zutreffend):		Full name of sixth joint inventor, if any:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).

McCormick, Paulding & Huber LLP  
City Place II  
185 Asylum Street  
Hartford, Connecticut 06103-4102  
U.S.A.

Telephone: (860) 549-5290  
Telefax: (860) 527-0464

<u>Attorneys</u>	<u>Reg.Nos.</u>
Donald K. Huber	<u>18,686</u>
Theodore R. Paulding	<u>19,294</u>
John C. Hilton	<u>22,965</u>
Arthur F. Dionne	<u>23,093</u>
Frederick J. Haesche	<u>24,529</u>
John C. Linderman	<u>24,420</u>
J. Kevin Grogan	<u>31,961</u>
Richard R. Michaud	<u>40,088</u>
Daniel G. Mackas	<u>38,541</u>
Peter J. Rainville	<u>41,263</u>
Marina F. Cunningham	<u>38,419</u>
Susan C. Oygard	<u>42,969</u>
Nicholas J. Tuccillo	<u>44,322</u>
Stephen P. Scuderi	<u>42,136</u>
Wm. Tucker Griffith	<u>44,726</u>

15